



Office *of the* Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's
Internal Controls over Issuing and
Monitoring Contractors' Homeland
Security Presidential Directive-12
Credentials

A-15-11-11178 | April 2013

MEMORANDUM

Date: April 18, 2013

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Internal Controls over Issuing and Monitoring Contractors' Homeland Security Presidential Directive-12 Credentials (A-15-11-11178)

The attached final report presents the results of our audit. Our objective was to determine whether the Social Security Administration had appropriate and adequate internal controls over issuing and monitoring Agency contractors' Homeland Security Presidential Directive-12 credentials.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.



Patrick P. O'Carroll, Jr.

Attachment

The Social Security Administration's Internal Controls over Issuing and Monitoring Contractors' Homeland Security Presidential Directive-12 Credentials

A-15-11-11178



April 2013

Office of Audit Report Summary

Objective

To determine whether the Social Security Administration (SSA) had appropriate and adequate internal controls over issuing and monitoring Agency contractors' Homeland Security Presidential Directive-12 (HSPD-12) credentials.

Background

HSPD-12 requires that all Federal agencies develop and implement a mandatory, Government-wide standard of identification for Federal employees and contractors. The purpose of HSPD-12 is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. The Federal Information Processing Standard 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, established a standard for a PIV system based on secure and reliable forms of identification issued by the Government to its employees and contractors. Federal regulations require that contractors comply with HSPD-12 PIV requirements.

Our Findings

We reviewed the processes for SSA components involved in HSPD-12 suitability and credentialing. Overall, we determined that, in certain cases, SSA did not communicate the results of suitability determinations to the appropriate personnel, did not deactivate credentials timely or enforce the collection of credentials from terminated contractors. During our review, we found instances when SSA's components did not follow procedures for (1) terminating unsuitable contractors and ensuring investigations were complete, (2) cancelling terminated contractors' credentials, and (3) enforcing the collection and destruction of credential cards.

Our Recommendations

We recommend SSA:

1. Ensure all components involved in the HSPD-12 suitability and credentialing process effectively communicate unsuitable determinations, contractor terminations and changes in SSA contracts including Contract Officer Technical Representative changes.
2. Perform periodic reconciliations between the suitability and credentialing systems to determine whether unsuitable or terminated contractors have been terminated, their credentials cancelled, and their suitability determination is correct in all appropriate systems.
3. Ensure contractors who have been terminated outside of the normal system termination process are also cancelled in all systems.
4. Document its collection and destruction of terminated credentials in accordance with FIPS 201.

The Agency agreed with our recommendations.

TABLE OF CONTENTS

Objective.....	1
Background.....	1
SSA Components and Systems Involved in HSPD-12 PIV.....	1
Responsibilities of CPSPM.....	2
Responsibilities of OPSS	3
Results of Review	4
Procedures not followed for Terminating Unsuitable Contractors and Completing Investigations	4
Unsuitable Contractors Continued Working on SSA Contracts.....	4
Terminated Unsuitable Contractors with Active Credentials	5
Active Contractors with Discontinued OPM Investigations.....	5
Procedures not Followed for Cancelling Credentials of Terminated Contractors.....	6
Procedures for Collecting and Destroying Credentials not Enforced.....	7
Conclusions.....	8
Recommendations.....	9
Agency Comments.....	9
Appendix A – Scope and Methodology	A-1
Appendix B – Flowcharts and Narratives	B-1
Appendix C – Agency Comments.....	C-1
Appendix D – Major Contributors.....	D-1

ABBREVIATIONS

AIMS	Administrative Instruction Manual System
CERMS	Contractor Enrollment Request Management System
C.F.R.	Code of Federal Regulations
CMS	Card Management System
CO	Contracting Officer
COTR	Contracting Officer Technical Representative
CPSPM	Center for Personnel Security and Project Management
CSS	Contractor Suitability System
EDS	Enrollment System
EPECS	Electronic Personal Enrollment Credential System
FIPS	Federal Information Processing Standard
HSPD-12	Homeland Security Presidential Directive–12
IDMS	Identity Management System
MRM	Material Resources Manual
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSS	Office of Protective Security Services
PIV	Personal Identity Verification
SSA	Social Security Administration
SSASy	Streamlined Acquisition System

OBJECTIVE

The objective of this audit was to determine whether the Social Security Administration (SSA) had appropriate and adequate internal controls over issuing and monitoring Agency contractors' Homeland Security Presidential Directive-12 (HSPD-12) credentials.

BACKGROUND

HSPD-12¹ requires that all Federal agencies develop and implement a mandatory, Government-wide standard of identification for Federal employees and contractors. The purpose of HSPD-12 is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.

To satisfy the HSPD-12 requirements, the National Institute of Standards and Technology issued Federal Information Processing Standard 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*.² FIPS 201 established a standard for a PIV system based on secure and reliable forms of identification the Government issues to its employees and contractors. Once the PIV process is complete, an individual's identity credentials are loaded onto a smart card called a PIV card or credential. The smart card contains stored identity credentials, such as a photograph, fingerprint, and other personal information, so the cardholder's identity can be electronically verified against the stored credentials. It functions as a visual identification for physical access and as an automated identity verification for computer systems access.

Federal regulations³ require that contractors comply with the requirements of HSPD-12 PIV. According to SSA policy, anyone requiring unescorted physical access to SSA facilities or access to SSA information systems for any period of time must go through the HSPD-12 PIV process to receive a credential.⁴

SSA Components and Systems Involved in HSPD-12 PIV

SSA's Center for Personnel Security and Project Management (CPSPM) and Office of Protective Security Services (OPSS) are involved in the PIV process. CPSPM conducts and oversees background investigations for SSA employees, contractors, students, volunteers and other

¹ HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

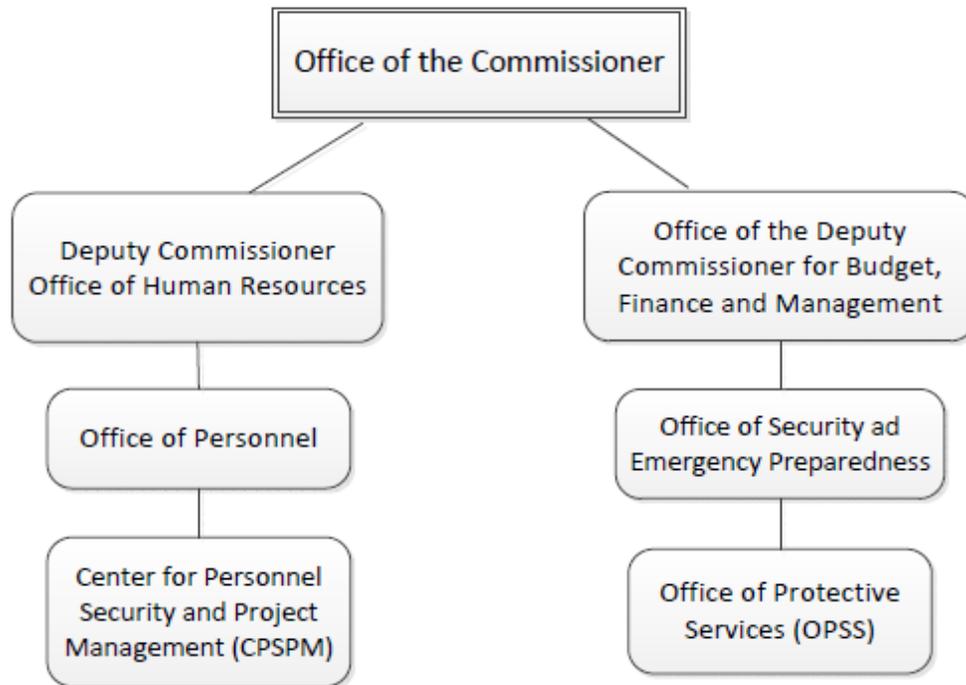
² FIPS Publication 201-1, *PIV of Federal Employees and Contractors*, National Institute of Standards and Technology, March 2006.

³ 48 C.F.R. § 52.204-9(a).

⁴ Administrative Instructions Manual System (AIMS) Material Resources Manual (MRM) 04.51.05 and SSA Memorandum, Contractor Enrollment Request Management System (CERMS), October 8, 2008.

individuals requiring frequent access to SSA facilities or logical systems. OPSS implements and manages the HSPD-12 process and FIPS 201 requirements. These two offices have different chains of command, as illustrated in Figure 1.

Figure 1: Components Involved HSPD-12 PIV



Responsibilities of CPSPM

CPSPM is responsible for ensuring all contractors receive the appropriate personnel suitability background investigation required by Federal laws and regulations.⁵ This includes making suitability determinations and ensuring determinations are appropriately recorded in the system. Once the process is complete, CPSPM notifies the Contracting Officer Technical Representative (COTR), the Contracting Officer (CO) and the contractor employer of the suitability adjudication by an automated suitability determination letter.

The suitability investigation provides a basis for the Agency’s suitability determination. Federal regulation⁶ states that the suitability determination is “. . . based on a person’s character or conduct that may have an impact on the integrity or efficiency of service.” Certain factors are considered in determining suitability, including misconduct or negligence in employment,

⁵ 48 C.F.R. § 52.204-9(a).

⁶ 5 C.F.R. § 731.101(a).

criminal or dishonest conduct, and fraud.⁷ SSA stated that contract employees are investigated at the same risk level as Federal employees who perform the same type of work.

Once the contractor submits the application paperwork to SSA, CPSPM conducts an initial background check, including a fingerprint check, verification of social security number, selective service registration, work authorization or citizenship and education, if indicated. CPSPM makes an initial suitability determination based on the results of this background check. CPSPM sends a letter stating the initial suitability determination to the COTR, the CO and the contractor employer. Suitable contractors may begin work on an SSA contract. CPSPM must also record the suitability determination into the Identity Management System (IDMS) to initiate the creation of a credential. Only CPSPM has the authority to enter the suitability determination into IDMS.

After making the initial determination, CPSPM sends the contractor's paperwork to the Office of Personnel Management (OPM). OPM performs a more in-depth background investigation, including verifying employment, checking credit references, and contacting references. Generally, OPM conducts investigations for SSA's contract employees.

Once OPM completes its background investigation, it sends CPSPM its results. CPSPM's initial suitability determination is the final determination unless the results of the OPM investigation cause CPSPM to change the suitability determination. If CPSPM determines the contractor to be unsuitable based on OPM's findings, CPSPM prepares a second letter for the COTR, the CO and the contractor employer stating that the contractor is unsuitable and must be removed from the contract immediately. OPSS stated that the COTR should contact OPSS to ensure the credential is deactivated within 18 hours of notification as required by FIPS 201.

CPSPM developed the Contractor Suitability System (CSS) to manage and maintain contractor background and suitability investigation information. CSS is for the sole use of CPSPM. It derives SSA contract information from SSA's Streamlined Acquisition System (SSASy). However, there are certain contracts not maintained in SSASy; these must be entered and updated manually by CPSPM.

Responsibilities of OPSS

OPSS led the Agency's implementation of HSPD-12. OPSS directs SSA's physical and protective security program and establishes policy to ensure the safety and security of SSA employees, visitors, and property.

As a requirement of FIPS 201, OPSS created IDMS, which maintains all enrollment and credentialing information required for PIV. IDMS has two components: the enrollment process and Card Management System (CMS). CPSPM enters and approves employees and contractors in IDMS, and OPSS maintains the creation of the HSPD-12 credential card and credential access

⁷ 5 C.F.R. § 731.202(b)(1)(2) and (3).

in CMS. Once the PIV process is complete and a contractor is determined suitable for work, OPSS issues an HSPD-12 credential.

As part of the enrollment process, OPSS developed the Contractor Enrollment Request Management System (CERMS) application for SSA COTRs to enter new contractors or remove existing contractors from contracts. CERMS notified authorized personnel to issue or revoke credentials to SSA contractors. The Electronic Personal Enrollment Credential System (EPECS) replaced CERMS on February 24, 2012. EPECS provides a higher level of security than CERMS and a more efficient contractor management process for COTRs.

RESULTS OF REVIEW

CPSPM and OPSS have separate responsibilities for implementing the requirements of HSPD-12. We reviewed the processes for each office as they related to HSPD-12 suitability and credentialing. During our review, we found instances when SSA's components did not follow procedures for (1) terminating unsuitable contractors and ensuring investigations were complete, (2) cancelling terminated contractors' credentials, and (3) enforcing the collection and destruction of credential cards.

Procedures not followed for Terminating Unsuitable Contractors and Completing Investigations

SSA facilities and systems are put at risk when unsuitable contractors and their credentials are not terminated immediately. According to SSA policy,⁸ if a contractor has received an unsuitable adjudication, CPSPM must inform the COTR, CO and the contractor employer of the action, and the Agency is responsible for immediately cancelling the contractor's credential. During our review, we found two contractors working on SSA contracts for longer than 1 year after an unsuitable determination. There were also unsuitable contractors who had been terminated from a contract, but their credentials were not cancelled timely. Additionally, contractors with incomplete or discontinued investigations continued to work on SSA contracts.

Unsuitable Contractors Continued Working on SSA Contracts

We reviewed a population of 6,057 contractors to determine whether there were unsuitable contractors with active credentials during our audit period. For all contractors identified as unsuitable, we checked IDMS for HSPD-12 credentials. We identified three contractors who had unsuitable determinations and active HSPD-12 credentials. Based on its initial background check, CPSPM approved these contractors for work on an SSA contract, and OPSS issued an HSPD-12 credential. However, based on the full OPM investigation, CPSPM's final determination for them was unsuitable.

⁸ AIMS MRM, 04.51.05 D.1.

Two of the three unsuitable contractors were still active on separate SSA contracts. One of the contractors was working as a senior IT engineer, and the other was working on a construction contract. Both contractors continued working on the contracts because the COTRs did not receive a letter stating the final unsuitable determination. CPSPM could not verify an unsuitable determination letter was sent to the COTR or contracting officer in these cases. One contractor was adjudicated unsuitable on July 20, 2011 and the other on August 17, 2011. Based on our audit work, both contractors were terminated and their credentials cancelled on September 14, 2012. A third contractor, who was providing IT support services, continued working on an SSA contract for 25 days after the unsuitable determination. This contractor resigned in 2011 for reasons unrelated to his suitability; however, reinstatement on the contract was possible for up to 1 year since the COTR was not informed of an unsuitable adjudication.

OPSS and other IDMS users depend on the system's validity when making decisions affecting access approval. During our fieldwork, we found 10 unsuitable contractors out of the same contractor population, including the 3 noted above, who still had a favorable suitability status in the IDMS. OPSS stated they were not notified of a change in the contractors' final suitability determinations from suitable to unsuitable. Contractors with suitable determinations in IDMS can have their physical and system access reinstated within 1 year after they stop working on the contract without going through the PIV process again. Therefore, it is imperative that the suitability information in IDMS be correct.

Our review noted SSA did not follow procedures for terminating three unsuitable contractors. During our review, we reconciled the suitability information in CSS with the information in IDMS. CPSPM and OPSS could periodically conduct a similar reconciliation to ensure unsuitable contractors are terminated and their credentials cancelled.

Terminated Unsuitable Contractors with Active Credentials

Physical access controls provide assurance that SSA's facilities are secure. FIPS 201 requires that the credential of an unsuitable contractor be cancelled within 18 hours of notification. During our review, we noted three unsuitable contractors, included in the 10 contractors noted above, had been terminated from the SSA contracts; however, their credential access was not cancelled for 11 months, 6 months, and 83 days, respectively. Two of the three were working as security guards in SSA facilities; their credential access was not cancelled for 11 months and 83 days after their terminations due to an unsuitable determination. The third contractor was providing janitorial services; his credential access was cancelled 6 months after his termination.

OPSS maintains that, in most cases, it cancels a credential within 4 hours of notification from the COTR. We were unable to verify why it took so long to cancel these credentials. It could be the result of poor communication between OPSS and the COTRs or OPSS' failure to cancel the credential according to policy. Weak controls over credential termination compromise the security of SSA facilities and employees.

Active Contractors with Discontinued OPM Investigations

We selected a probe sample of 25 contractors who had active credentials but did not appear to have suitability investigations. We found three contractors who had active HSPD-12 credentials,

but their OPM investigations were not completed. CPSPM told us that when OPM returns a file with an incomplete investigation, CPSPM gathers the missing information and sends the file back to OPM for completion. CPSPM stated that a returned file does not necessarily indicate an applicant is unsuitable; a file could be returned because of missing information. Even though CPSPM could not produce suitability letters for these contractors, all three were issued HSPD-12 credentials.

- In 2009, while conducting an initial background investigation, CPSPM found one contractor had an arrest. CPSPM requested additional information from the contractor and received no response. CPSPM then discontinued the investigation due to noncompliance. However, the contractor was issued a credential and was working on an IT services contract at the time of our fieldwork. As a result of this finding, CPSPM was conducting a new investigation and, based on the preliminary background check, determined the contractor is suitable to continue working pending the full OPM investigation.
- CPSPM could not explain why the OPM investigations were halted for the other two contractors. Both contractors were working on IT contracts. One of these contractors resigned from the contract in July 2011. The other accepted a position as an SSA employee in August 2012 and was undergoing an employee background investigation at the time of this review.

CPSPM was unable to confirm why these two investigations remained incomplete. OPSS and the COTRs told us they were not informed of a discontinued investigation so the contractors continued working on SSA contracts. SSA facilities and systems could be at risk when a contractor is allowed to continue working without a complete OPM background investigation.

Procedures not Followed for Cancelling Credentials of Terminated Contractors

FIPS 201 requires that all changes in the credential holder's status be reflected in the system within 18 hours of notification. For example, when a contractor no longer requires access to SSA or their employment on a contract is terminated, the HSPD-12 credential and electronic certificates it contains must be revoked within 18 hours of notification. We found weaknesses in the procedures for cancelling credentials of terminated contractors.

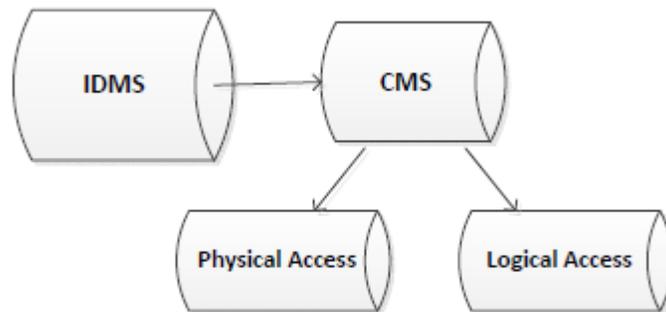
To determine whether contractors with active credentials were still working on an SSA contract, we selected 50 suitable contractors who had active credentials during our review period. We requested that the SSA COTR and contractors' employers verify that contractors were still working on an SSA contract. We determined 7 of the 50 contractors had terminated an SSA contract either before or during our audit period, but they still had active credential cards with physical access enabled.

We selected 50 suitable contractors whose credentials were cancelled during our review period. We requested that the SSA COTR verify that the contractor had terminated an SSA contract during the period. We found 11 of the 50 contractors had terminated an SSA contract, but their HSPD-12 credentials were not deactivated within 18 hours. Based on our review, these were suitable contractors who left their respective contracts for reasons other than suitability. We noted their credentials were not deactivated for 13 days to 1 year from the date of termination.

OPSS told us the COTR must notify OPSS if a contractor has terminated the contract so physical access can be terminated within 18 hours of the contractor termination. However, in these cases, we could not determine whether the COTRs neglected to notify OPSS of the contractor termination or the COTR notified OPSS of a contractor termination, but OPSS neglected to cancel the credential within 18 hours.

We also found 6 of the 50 contractors whose credentials were cancelled had stopped working on an SSA contract but still had HSPD-12 credentials with physical access. We asked OPSS to explain how contractors with physical access were included in our terminated contractor sample population. OPSS told us that when physical access needs to be terminated immediately, credentials can be deactivated outside of the system process. Deactivation generally occurs in IDMS, which triggers deactivation in CMS. CMS has two subsystems: one for physical access and another for logical access (see Figure 2). Deactivation would automatically take place in these subsystems. However, OPSS can deactivate a contractor's access in one subsystem, which bypasses the system process that deactivates access in all systems. OPSS must then manually cancel access in all other systems and subsystems. For 6 of the 50 contractors who terminated but still had physical access, OPSS had not cancelled access in all systems.

Figure 2: HSPD-12 Access Systems



Procedures for Collecting and Destroying Credentials not Enforced

According to FIPS 201, normal termination procedures must be in place to ensure contractor credential cards are collected and destroyed. SSA⁹ guidance instructs supervisors or project officers to contact the HSDP-12 help desk within 18 hours of a contractor's separation to terminate physical and logical access and render the card unreadable.

We selected a sample of 50 contractors who were terminated during the audit period and asked the COTRs and OPSS to verify the contractors' credential cards had been collected and destroyed.

⁹ AIMS MRM, 04.51, *Personal Identity Verification and Credential Issuance Process*.

- For 40 of the 50 contractors, the COTRs told us they collected the terminated credential cards; however, there was no record the credential card had been collected and destroyed. OPSS also could not verify the collection and destruction of the cards.
- For 8 of the 50 contractors, the COTRs told us they were unable to collect the contractors' credential cards. OPSS could not tell us whether these cards were collected.
- For 2 of the 50 contractors, the COTR could not be located for inquiry because of outdated contract information in SSA systems.

OPSS did not maintain a record of returned credential cards. Therefore, it cannot confirm that a specific credential had been collected and destroyed; they could only confirm the credential had been deactivated in the system. OPSS told us deactivating credentials in the system is the prevailing control because it destroys the card's electronic authentication, which will prevent an unauthorized person from entering an SSA building where a card reader has been installed. At the time of our review, card readers had been installed at SSA Headquarters, the National Computer Center, and most of the outlying SSA buildings. However, we found one building where no card reader was installed at either of the two entrances and another building where there was a card reader at the main entrance but not at the side entrance. At a third location, a security guard told us the card readers were not working at one entrance so they were not being used at either of the two entrances.

Additionally, HSPD-12 is a Government-wide identification and can be used to enter other Federal facilities. In Federal facilities that do not have card readers, credentials may be used for visual identification only. Thus, any SSA-terminated contractor still holding a credential could gain access to Federal buildings that do not have card readers. The deactivation and collection of terminated credential cards provides greater assurance that terminated contractors cannot enter secured facilities.

CONCLUSIONS

Our audit work identified vulnerabilities in the HSPD-12 suitability and credentialing processes at SSA. Overall, our review determined that SSA did not have adequate internal controls over issuing and monitoring HSPD-12 credentials. During our review, we found instances when SSA's components did not follow procedures for (1) terminating unsuitable contractors and ensuring investigations were complete, (2) cancelling terminated contractors' credentials, and (3) enforcing the collection and destruction of credential cards.

Contractor suitability determinations are made to prevent unsuitable contractors from accessing SSA facilities and sensitive information. In a few cases, we determined that OPSS and COTRs were not always informed of the results of unsuitable determinations. This resulted in three unsuitable contractors who continued to work on SSA contracts after they had been given an unsuitable determination. Two of the three worked on SSA contracts for over 1 year after an unsuitable determination. CPSPM must record the suitability determination into the IDMS to initiate the creation of a credential. Since the system allows or denies access based on suitability, it is crucial that the IDMS reflect the correct suitability determination to ensure unsuitable contractors cannot access SSA buildings. During the course of this review, OPSS began

replacing the IDMS with the Electronic Personal Enrollment and Credentialing System (EPECS). EPECS provides CPSPM and COTRs additional tools and functionality for updating contractor status following an initial suitability determination and throughout the lifetime of the credential. These additional tools, while still dependent on solid business processes for communicating an individual's suitability status to the COTR, CO, contracting company and OPSS, provide CPSPM the ability to revoke logical and physical access immediately, but not later than 18 hours after notification of an unsuitable adjudication.

Weaknesses in the controls over credential cancellation of terminated contractors compromise the security of SSA facilities and employees. We found terminated contractor credentials with active physical access and credentials that were not deactivated within 18 hours of termination. Also, we found that in some cases, OPSS bypassed the normal system process to deactivate credentials. OPSS did not manually cancel access in all other subsystems as required so access information was incorrect in certain subsystems. Additionally, COTRs are responsible for communicating changes to contractor employment. If COTRs do not provide notification of a contractor termination, the contractor status may be incorrect in the system.

According to FIPS 201, normal termination procedures must be in place to ensure contractor credential cards are collected and destroyed. OPSS did not maintain a record of returned credential cards. Therefore, it could not confirm a specific credential had been collected and destroyed only that it had been deactivated in the system.

RECOMMENDATIONS

To ensure SSA facilities and property are properly secured and safeguarded, SSA needs assurance that controls over HSPD-12 suitability and credentialing are followed and enforced. Therefore, we recommend SSA:

1. Ensure all components involved in the HSPD-12 suitability and credentialing process effectively communicate unsuitable determinations, contractor terminations and changes in SSA contracts including COTR changes.
2. Perform periodic reconciliations between the suitability and credentialing systems to determine whether unsuitable or terminated contractors have been terminated, their credentials cancelled, and their suitability determination is correct in all appropriate systems.
3. Ensure contractors who have been terminated outside of the normal system termination process are also cancelled in all systems.
4. Document its collection and destruction of terminated credentials in accordance with FIPS 201.

AGENCY COMMENTS

The Agency agreed with our recommendations. The Agency's complete comments are included in Appendix C.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objectives, we:

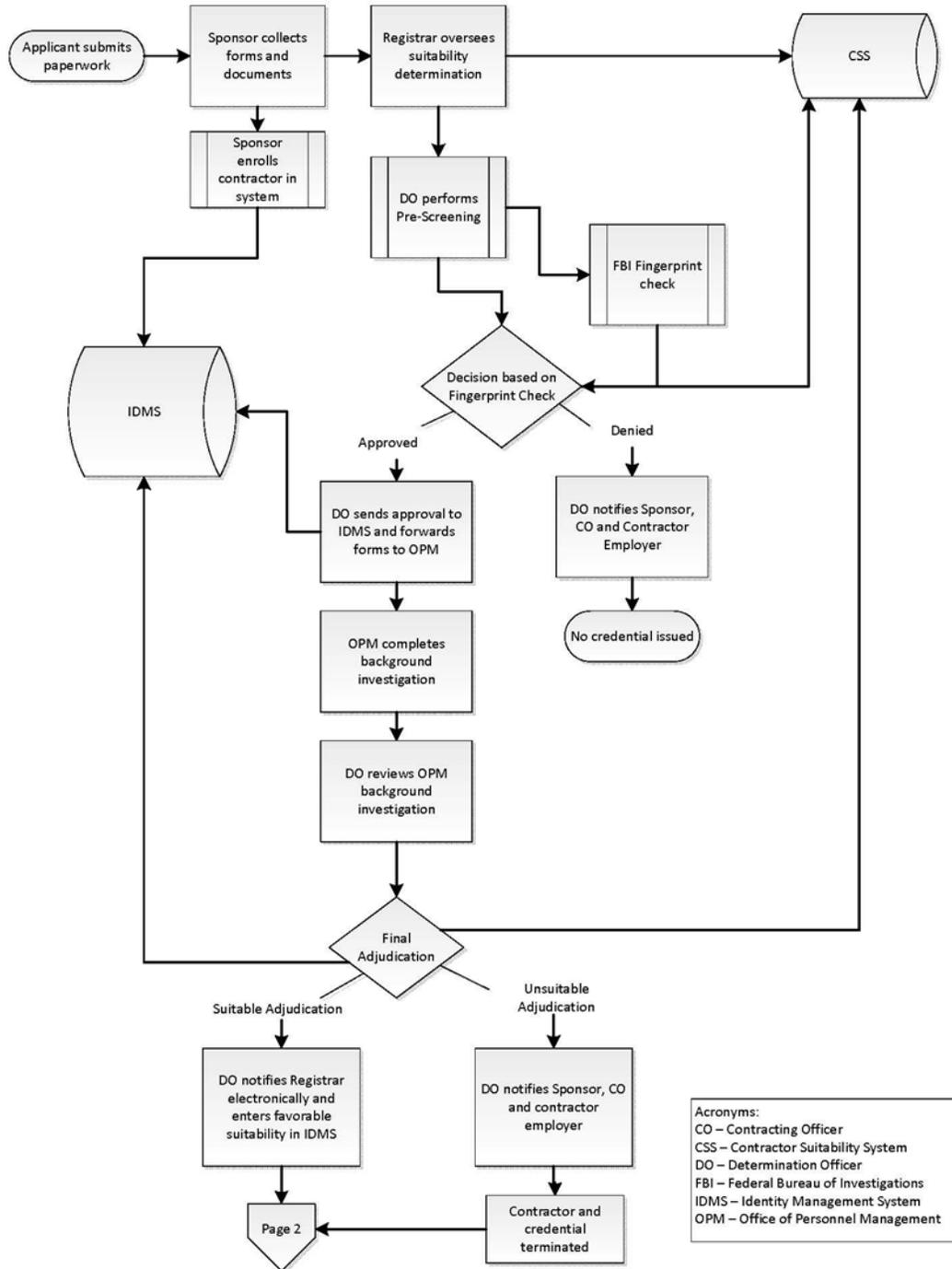
- Reviewed the Presidential Directive, Federal regulations, and Office of Management and Budget memorandums related to the implementation of Homeland Security Presidential Directive-12 (HSPD-12).
- Reviewed Federal Information Processing Standard 201-1 and Administrative Instruction Manual System guidance on personal identity verification and the credential issuance process.
- Interviewed management and staff from the Center for Personnel Security and Project Management and Office of Protective Security Services to gain an understanding of the processes and controls related to HSPD-12 suitability and credentialing.
- Observed the system screens and processes for enrolling, approving, and issuing an HSPD-12 credential.
- Obtained suitability data for all current or terminated contractors from the Contractor Suitability System (CSS) for the audit period.
- Obtained credential data for all current or terminated contractors from Identity Management System (IDMS) for the audit period.
- Performed a reconciliation of contractor data between the CSS and IDMS and tested samples to ensure controls and procedures were followed.
- Reviewed a sample of contractor background investigation files for completeness.
- Observed card readers at Agency buildings in Woodlawn.

We determined the computerized data used during our review were sufficiently reliable given our objectives, and the intended use of the data should not lead to incorrect or unintentional conclusions.

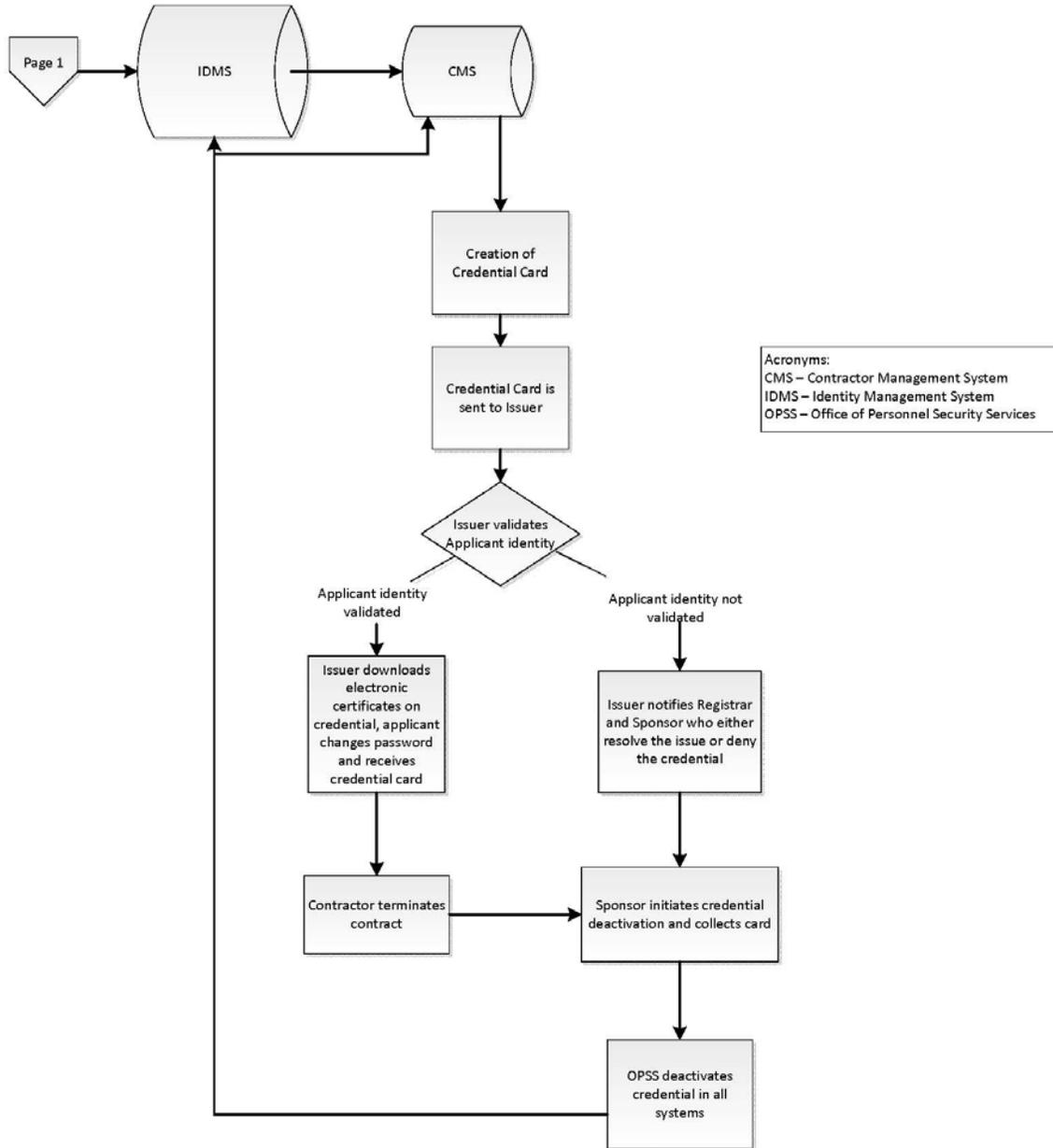
We performed our fieldwork at Headquarters in Baltimore, Maryland, from October 2011 through September 2012. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusion based on our audit objectives

Appendix B – FLOWCHARTS AND NARRATIVES

Contractor Suitability and Enrollment Processes



Card Issuance Process



Personal Identity Verification

The Personal Identification Verification (PIV) credential is personalized with identity information about the individual to whom the card is issued. FIPS 201 creates a structured process for sponsoring and processing individuals in the PIV system and for issuing credentials. The process calls for “trusted individuals” who are vetted, trained, and certified for specific roles to ensure a separation of duties throughout the process. This is to ensure that no single individual can corrupt the system and issue a credential. The specific roles within the process are as follows.

- **Applicant** - An employee, contractor, or other individual requiring access to a Government facility or system.
- **Sponsor** – The Sponsor (COTR) is responsible for initiating the HSPD-12 enrollment of the employee or contractor applicant. The Sponsor is responsible for
 - entering the applicant’s personal and work information,
 - collecting the biometric identity of applicants through a fingerprint scan,
 - capturing the applicant’s picture, and
 - scanning the applicant’s identity documents.
- **Registrar** - The Registrar (CPSM) conducts a Numident check to validate the applicant’s identity and ensure the identity documents are authentic.
- **Determination Officer (DO)** – The DO (CPSM) ensures an appropriate background investigation is initiated and makes a final suitability determination. The DO also verifies and inputs the date and results of the fingerprint check in IDMS.
- **Issuer** - The Issuer (OPSS) issues the credential to an applicant after completing the following.
 - Verify Identity of the Applicant in relation to the Sponsor’s input of the identity document.
 - Verify the Biometric Identity of the Applicant through a Fingerprint Scan.
 - Activate the Credential in CMS.
 - Assist the Applicant in applying the six to eight-digit personal identification number to the credential.

PIV Process Flow

The PIV process begins when the contractor applicant completes either a Form SF-85 (*Questionnaire for Non Sensitive Positions*) or a Form SF-85P (*Questionnaire for Public Trust Positions*). The applicant provides SSA with these Forms along with a *Fair Credit Report Authorization* (FCRA), an OF 306 form (*Declaration for Federal Employment*), two completed

FD-258 fingerprint cards and two I-9 identity documents. An Applicant who is a non-citizen must also provide work authorization forms. If an applicant claims to have had a background investigation from another Federal agency, CPSPM will verify the investigation with the Office of Personnel Management (OPM). If a higher level background investigation is required for the current contract than is on record, CPSPM will require that the applicant complete paperwork for the higher level investigation. The CPSPM conducts a prescreen background check which includes a National Criminal Investigations Center (NCIC) check, verification of Social Security number, citizenship check, and check for Selective Service System registration, where applicable.

Based on the results of the prescreen background check, CPSPM will issue either a suitable or unsuitable determination letter to the contractor employer, SSA Contracting Officer (CO), and Sponsor (COTR). If the suitability determination is favorable, the Sponsor (COTR) is responsible for entering the applicant's information into EPECS (previously CERMS). The Registrar/DO will verify all information. The DO enters the suitability determination in IDMS, which approves credential issuance. The Issuer issues a temporary credential and sends an electronic message to the credential manufacturer to print a credential. This allows the contractor to begin work while a full background investigation is completed by OPM.

Once the Issuer receives the printed credential card, the applicant appears before the Issuer with his/her I-9 identification documents that were presented at the beginning of the process. The Issuer validates the actual identification against the picture identification, compares I-9 documents, and electronically compares the Applicant's fingerprints to those in IDMS. The Issuer downloads the electronic certificates onto the credential, and the applicant changes his or her password in the system. The Issuer signs the credential finalizing the credential process and gives the credential to the Applicant. If the identification check fails, the Issuer notifies the Registrar and Sponsor who either resolve the identification issue or deny the credential to the Applicant.

Once the OPM investigation is complete, the investigative report is submitted to the DO for adjudication. If the DO's final adjudication is suitable, the contractor continues to perform SSA contract work and no further action is required. If the final adjudication is unsuitable, CPSPM issues an unsuitable letter to the contractor employer, CO and COTR. The COTR is responsible for ensuring the contractor is removed from the contract, notifying OPSS to cancel the credential and collecting the contractor's credential.

Appendix C – AGENCY COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: March 28, 2013 Refer To: SIJ-3

To: Patrick P. O’Carroll, Jr.
Inspector General

From: Katherine Thornton /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, “The Social Security Administration’s Internal Controls over Issuing and Monitoring Contractors’ Homeland Security Presidential Directive-12 Credentials” (A-15-11-11178)—INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

**COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT,
“THE SOCIAL SECURITY ADMINISTRATION’S INTERNAL CONTROLS OVER
ISSUING AND MONITORING CONTRACTORS’ HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE (HSPD)-12 CREDENTIALS” (A-15-11-11178)**

Recommendation 1

Ensure all components involved in the HSPD-12 suitability and credentialing process effectively communicate unsuitable determinations, contractor terminations, and changes in SSA contracts, including COTR changes.

Response

We agree. The Office of Security and Emergency Preparedness’ Office of Protective Security Services and the Office of Personnel’s Center for Personnel Security and Project Management are developing a Memorandum of Understanding to document, in detail, the communication responsibilities of all parties involved in the contractor issuance and revocation processes for HSPD-12 credentials. In addition, we fully implemented the automated Electronic Personal Enrollment and Credentialing System (EPECS) on February 24, 2013.

EPECS provides a higher level of security than our previous credentialing system and a more efficient contractor management process for the Contracting Officer Technical Representatives. EPECS provides additional tools and functionality for updating contractor status following an initial suitability determination and throughout the lifetime of the credential. We are updating the related Administrative Instruction Manual System Guide (AIMS), Material Resources Manual 04.51, “Personal Identity Verification and Credential Issuance Process,” to reflect all parties’ roles and responsibilities within the new system.

Recommendation 2

Perform periodic reconciliations between the CSS and IDMS systems to determine whether unsuitable or terminated contractors have been terminated, their credentials cancelled, and their suitability determination is correct in all appropriate systems.

Response

We agree. We replaced the Identity Management System (IDMS) with EPECS. We will ensure periodic reconciliation between EPECS and the Common System Services, as it may add value to the current business process.

Recommendation 3

Ensure contractors who have been terminated outside of the normal system termination process are also cancelled in all systems.

Response

We agree.

Recommendation 4

Document its collection and destruction of terminated credentials in accordance with FIPS 201.

Response

We agree. We will determine the most cost-effective and time-sensitive approach for tracking the collection and destruction of terminated credentials.

Appendix D – MAJOR CONTRIBUTORS

Victoria Vetter, Director, Financial Audit Division

Judith Kammer, Audit Manager, Financial Audit Division

Kali Biagioli, Senior Auditor, Financial Audit Division

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (<http://oig.ssa.gov/>) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "[Beyond The Numbers](#)" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.



[Watch us on YouTube](#)



[Like us on Facebook](#)



[Follow us on Twitter](#)



[Subscribe to our RSS feeds or email updates](#)

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at <http://oig.ssa.gov/audits-and-investigations/audit-reports/all>. For notification of newly released reports, sign up for e-updates at <http://oig.ssa.gov/e-updates>.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website: <http://oig.ssa.gov/report-fraud-waste-or-abuse>

Mail: Social Security Fraud Hotline
P.O. Box 17785
Baltimore, Maryland 21235

FAX: 410-597-0118

Telephone: 1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time

TTY: 1-866-501-2101 for the deaf or hard of hearing